SCADA Systems

Brandon Braxton
CYSE 200T: Cybersecurity, Technology, And Society
Professor Chris Bowman
JUNE 28, 2026

Supervisory Control and Data Acquisition (SCADA) systems serve as the backbone to most critical infrastructure systems such as power grids, water treatment facilities, ships and manufacturing plants. Consequentially, their security should be prioritized and higher than any other technology sector. SCADA systems have the following subsystems: “the apparatus used by a human operator,” “a supervisory system that gathers all the required data about the process,” “Remote Terminal Units (RTUs)…which help convert sensor signals to digital data and send the data to the supervisory stream,” “PLCs used as field devices,” and communication infrastructure connecting the RTUs to the supervisory system (SCADA Systems, n.d.). SCADA architecture has progress through three generations – Monolithic, Distributed and Networked. In the present generation, Networked, “communication between the system and the master station is done through the WAN protocols lie the Internet Protocols (IP)” (SCADA Systems, n.d.).

Like other forms of technology, SCADA also faces different types of vulnerabilities. “Common vulnerabilities in these systems include unpatched software, insecure remote access, weak authentication mechanisms, lack of network segmentation, and physical tampering” (Cybersecurity of Critical Infrastructure With ICS/SCADA Systems – IEEE Public Safety Technology, n.d.). Being that the current generation is networked using IP protocols, any devices that may connect to the WAN or LAN that are not regularly patched, or if the user has become victim to a phishing attack, it leaves the SCADA system vulnerable. Another potential vulnerability is an insider threat, where someone within the company make intentional harmful changes to the system.

A couple of ways to mitigate some of the vulnerabilities would be regular patching cycles for all devices and implementing the AAA model – Authenticate, Authorize, Account. The user would have first identify themselves using an employee ID and another form of identification, then there could be a check-in station or server to check the user’s access to the SCADA system then each change would be logged and reviewed.

References

SCADA Systems. (n.d.). Retrieved June 21, 2026, from http://www.scadasystems.net

Cybersecurity of Critical Infrastructure with ICS/SCADA Systems – IEEE Public Safety Technology. (n.d.). https://publicsafety.ieee.org/topics/cybersecurity-of-critical-infrastructure-with-ics-scada-systems/